लेजिसलेटिव ब्रीफ

डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2023

डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2023 को लोकसभा में 3 अगस्त, 2023 को पेश किया गया।

साकेत सूर्य
saket@prsindia.org

4 अगस्त, 2023

बिल की मुख्य विशेषताएं

- बिल भारत के भीतर डिजिटल पर्सनल डेटा की प्रोसेसिंग पर लागू होता है जहां यह डेटा ऑनलाइन जमा किया जाता है या ऑफलाइन जमा किया जाता है और फिर उसे डिजिटलीकृत किया जाता है। यह भारत के बाहर पर्सनल डेटा प्रोसेसिंग पर भी लागू होगा, अगर यह प्रोसेसिंग भारत में वस्तुओं और सेवाओं को ऑफर करने के लिए की जाती है।
- व्यक्ति की सहमति हासिल करने के बाद केवल वैध उद्देश्य के लिए पर्सनल डेटा को प्रोसेस किया जा सकता है। निर्दिष्ट वैध उपयोग के लिए सहमति की जरूरत नहीं होगी जैसे व्यक्ति द्वारा स्वेच्छा से डेटा को शेयर करना, या राज्य द्वारा परमिट, लाइसेंस, लाभ और सेवा प्रदान करने के लिए डेटा प्रोसेस करना।
- डेटा फिड्यूशरी डेटा की सटीकता को बनाए रखने, डेटा को सुरक्षित रखने और उद्देश्य पूरा होने के बाद डेटा को डिलीट करने के लिए बाध्य होगा।
- बिल व्यक्तियों को कुछ अधिकार देता है जैसे सूचना हासिल करने का अधिकार, डेटा को संशोधित और मिटाने की मांग करने का अधिकार और शिकायत निवारण।
- केंद्र सरकार राज्य की सुरक्षा, सार्वजनिक व्यवस्था और अपराधों की रोकथाम जैसे निर्दिष्ट आधार पर सरकारी एजेंसियों को बिल के प्रावधानों से छूट दे सकती है।
- केंद्र सरकार भारतीय डेटा प्रोटेक्शन बोर्ड की स्थापना करेगी जोकि बिल के प्रावधानों के गैर अनुपालन पर फैसला देगा।

प्रमुख मुद्दे और विश्लेषण

- राज्य को राष्ट्रीय सुरक्षा जैसे आधार पर डेटा प्रोसेसिंग संबंधी छूट से डेटा कलेक्शन, प्रोसेसिंग और रिटेंशन उससे अधिक हो सकता है, जितना जरूरी है। इससे प्राइवेसी के मौलिक अधिकार का उल्लंघन हो सकता है।
- बिल पर्सनल डेटा की प्रोसेसिंग से होने वाले नुकसान के जोखिम को रेगुलेट नहीं करता।
- बिल डेटा प्रिंसिपल को डेटा पोर्टेबिलिटी का अधिकार और भुला दिए जाने का अधिकार (राइट टु बी फॉरगॉटन) नहीं देता।
- बिल अधिसूचना के जरिए सरकार द्वारा प्रतिबंधित देशों को छोड़कर भारत के बाहर पर्सनल डेटा के ट्रांसफर की अनुमति देता है। यह व्यवस्था उन देशों में डेटा सुरक्षा मानकों का पर्याप्त मूल्यांकन सुनिश्चित नहीं कर सकती है जहां पर्सनल डेटा के ट्रांसफर की अनुमति है।
- भारतीय डेटा प्रोटेक्शन बोर्ड के सदस्यों को दो वर्षों के लिए नियुक्त किया जाएगा और वे दोबारा नियुक्ति के लिए पात्र होंगे। दोबारा नियुक्ति की गुंजाइश के साथ अल्पावधि का कार्यकाल बोर्ड के स्वतंत्र कामकाज को प्रभावित कर सकता है।

भाग क : बिल की मुख्य विशेषताएं

संदर्भ

पर्सनल डेटा वह सूचना होती है जोकि चिन्हित या चिन्हित करने योग्य व्यक्ति से संबंधित होती है। बिजनेस, साथ ही साथ सरकारी संस्थाएं वस्तुओं और सेवाओं की डिलिवरी के लिए पर्सनल डेटा को प्रोसेस करती हैं। पर्सनल डेटा की प्रोसेसिंग से व्यक्तियों की वरीयताओं को समझने में मदद मिलती है, और यह कस्टमाइजेशन, टार्गेटेड विज्ञापन और सुझावों को विकसित करने में मदद कर सकते हैं। पर्सनल डेटा की प्रोसेसिंग से कानून प्रवर्तन में भी सहायता मिल सकती है। अनियंत्रित प्रोसेसिंग से व्यक्तियों की प्राइवेसी पर प्रतिकूल प्रभाव पड़ सकता है। प्राइवेसी को मौलिक अधिकार के रूप में मान्यता दी गई है।[1] इससे व्यक्तियों को वित्तीय नुकसान, प्रतिष्ठा की हानि और प्रोफाइलिंग जैसी हानि हो सकती है।

वर्तमान में भारत में डेटा प्रोटेक्शन पर कोई अकेला कानून नहीं है। पर्सनल डेटा का रेगुलेशन इनफॉरमेशन टेक्नोलॉजी (आईटी) एक्ट, 2000 के तहत किया जाता है।[2,3] 2017 में केंद्र सरकार ने डेटा प्रोटेक्शन पर एक्सपर्ट कमिटी का गठन किया था जिसके अध्यक्ष जस्टिस बी.एन. श्रीकृष्ण थे। इस कमिटी के गठन का उद्देश्य देश में डेटा प्रोटेक्शन से संबंधित मामलों की समीक्षा करना था। कमिटी ने जुलाई 2018 में अपनी रिपोर्ट सौंपी।[4] कमिटी के सुझावों के आधार पर पर्सनल डेटा प्रोटेक्शन बिल, 2019 को दिसंबर 2019 में लोकसभा में पेश किया गया।[5] बिल को ज्वाइंट पार्लियामेंटरी कमिटी को भेजा गया जिसने दिसंबर 2021 में अपनी रिपोर्ट सौंपी।[2] अगस्त 2022 में बिल को संसद से वापस ले लिया। नवंबर 2022 में एक ड्राफ्ट बिल को सार्वजनिक परामर्श के लिए जारी किया गया।[6] अगस्त 2023 में संसद में डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2023 को पेश किया गया।[7]

मुख्य विशेषताएं

- **एप्लिकेबिलिटी**: बिल भारत के भीतर डिजिटल पर्सनल डेटा की प्रोसेसिंग पर लागू होता है जहां यह डेटा: (i) ऑनलाइन जमा किया जाता है या (ii) ऑफलाइन जमा किया जाता है और फिर उसे डिजिटलीकृत किया जाता है। यह भारत के बाहर पर्सनल डेटा प्रोसेसिंग पर भी लागू होगा, अगर यह प्रोसेसिंग भारत में वस्तुओं और सेवाओं को ऑफर करने के लिए की जाती है। पर्सनल डेटा किसी व्यक्ति के उस डेटा को कहा जाता है, जिससे वह व्यक्ति पहचाना जाता है, या जो उससे संबंधित होता है। प्रोसेसिंग उस पूर्ण या आंशिक ऑटोमेटेड ऑपरेशन या सेट ऑफ ऑपरेशंस को कहा जाता है जो डिजिटल पर्सनल डेटा पर किए जाते हैं। इसमें कलेक्शन, स्टोरेज, उपयोग और शेयरिंग शामिल है।
- **सहमति**: व्यक्ति की सहमति हासिल करने के बाद केवल वैध उद्देश्य के लिए पर्सनल डेटा प्रोसेस किया जा सकता है। सहमति लेने से पहले नोटिस देना होगा। नोटिस में जमा किए जाने वाले पर्सनल डेटा का विवरण और प्रोसेसिंग का उद्देश्य होना चाहिए। सहमति किसी भी समय वापस ली जा सकती है। 'वैध उपयोग' के लिए सहमति की जरूरत नहीं होगी, जिसमें निम्न शामिल हैं: (i) निर्दिष्ट उद्देश्य, जिसके लिए किसी व्यक्ति ने अपनी मर्जी से डेटा दिया है, (ii) सरकार द्वारा लाभ या सेवा का प्रावधान, (iii) मेडिकल इमरजेंसी और (iv) रोजगार। 18 वर्ष से कम उम्र के व्यक्तियों के लिए माता-पिता या लीगल गार्जियन की सहमति लेनी होगी।
- **डेटा प्रिंसिपल के अधिकार और कर्तव्य**: जिस व्यक्ति के डेटा को प्रोसेस किया जा रहा है (डेटा प्रिंसिपल), उसे निम्नलिखित का अधिकार होगा: (i) प्रोसेसिंग के बारे में जानकारी हासिल करना, (ii) पर्सनल डेटा में करेक्शन और उसे हटाने की मांग करना, (iii) मृत्यु या अक्षमता की स्थिति में किसी दूसरे को इन अधिकारों का इस्तेमाल करने के लिए नामित करना, और (iv) शिकायत निवारण। उन्हें: (i) झूठी या ओछी शिकायत दर्ज नहीं करानी चाहिए और (ii) कोई गलत विवरण नहीं देना चाहिए या निर्दिष्ट मामलों में किसी दूसरे का रूप नहीं धरना चाहिए। इन कर्तव्यों का उल्लंघन करने पर 10,000 रुपए तक का जुर्माना लगाया जाएगा।
- **डेटा फिड्यूशरी के दायित्व**: एंटिटी, प्रोसेसिंग के उद्देश्य और तरीके को निर्धारित करने वाली, (डेटा फिड्यूशरी) को निम्नलिखित करना चाहिए: (i) उसे डेटा की सटीकता और पूर्णता सुनिश्चित करने के लिए उचित प्रयास करने चाहिए, (ii) डेटा ब्रीच को रोकने के लिए उचित सुरक्षात्मक उपाय करने चाहिए, (iii) ब्रीच की स्थिति में भारतीय डेटा प्रोटेक्शन बोर्ड और प्रभावित व्यक्तियों को उसकी जानकारी देनी चाहिए, और (iv) उद्देश्य पूरा होने और लीगल उद्देश्यों के लिए रिटेंशन जरूरी न होने (स्टोरेज लिमिटेशन) पर पर्सनल डेटा को मिटा देना चाहिए। सरकारी संस्थाओं के मामले में, स्टोरेज लिमिटेशन और डेटा प्रिंसिपल का डेटा मिटाने का अधिकार लागू नहीं होगा।
- **भारत के बाहर पर्सनल डेटा ट्रांसफर करना**: बिल अधिसूचना के जरिए सरकार द्वारा प्रतिबंधित देशों को छोड़कर भारत के बाहर पर्सनल डेटा के ट्रांसफर की अनुमति देता है।
- **छूट**: डेटा प्रिंसिपल के अधिकार और डेटा फिड्यूशरी के दायित्व (डेटा सिक्योरिटी को छोड़कर) निर्दिष्ट मामलों में लागू नहीं होंगे। इनमें निम्नलिखित शामिल हैं: (i) अपराधों की रोकथाम और जांच, और (ii) कानूनी अधिकारों या दावों का प्रवर्तन। केंद्र सरकार, अधिसूचना के जरिए, कुछ निश्चित गतिविधियों को बिल के प्रावधानों से छूट दे सकती है। इनमें निम्नलिखित शामिल हैं: (i) राज्य की सुरक्षा और सार्वजनिक व्यवस्था के हित में सरकारी एंटिटीज़ की ओर से होने वाली प्रोसेसिंग, और (ii) अनुसंधान, आर्काइविंग या स्टैटिस्टिकल उद्देश्य।
- **भारतीय डेटा प्रोटेक्शन बोर्ड**: केंद्र सरकार भारतीय डेटा संरक्षण बोर्ड की स्थापना करेगी। बोर्ड के प्रमुख कार्यों में निम्नलिखित शामिल हैं: (i) अनुपालन की निगरानी करना और जुर्माना लगाना, (ii) डेटा ब्रीच की स्थिति में डेटा फिड्यूशिरीज़ को जरूरी उपाय करने का निर्देश देना, और (iii) प्रभावित व्यक्तियों द्वारा की गई शिकायतों को सुनना। बोर्ड के सदस्यों की नियुक्ति दो साल के लिए की जाएगी और वे पुनर्नियुक्ति के पात्र होंगे। केंद्र सरकार बोर्ड के सदस्यों की संख्या और चयन प्रक्रिया जैसे विवरण निर्धारित करेगी। बोर्ड के निर्णयों के खिलाफ टीडीसैट में अपील की जाएगी।
- **सजा**: बिल की अनुसूची विभिन्न अपराधों के लिए जुर्माना निर्दिष्ट करती है जैसे: (i) बच्चों से संबंधित दायित्वों को पूरा न करने पर 200 करोड़ रुपए और (ii) डेटा ब्रीच रोकने के लिए सुरक्षात्मक उपाय न करने पर 250 करोड़ रुपए। जांच के बाद बोर्ड सजा देगा।

भाग ख: प्रमुख मुद्दे और विश्लेषण

राज्य को छूट से प्राइवेसी पर प्रतिकूल प्रभाव पड़ सकता है

बिल: क्लॉज 7, 17, चैप्टर II, चैप्टर III

राज्यों द्वारा पर्सनल डेटा प्रोसेसिंग को बिल के तहत कई छूट दी गई हैं। संविधान के अनुच्छेद 12 के अनुसार राज्य में निम्नलिखित शामिल हैं: (i) केंद्र सरकार, (ii) राज्य सरकार, (iii) स्थानीय निकाय, और (iv) सरकार द्वारा गठित अथॉरिटी और कंपनियां। इन छूटों के साथ कई मुद्दे हो सकते हैं।

बिल के कारण राज्यों द्वारा अनियंत्रित डेटा प्रोसेसिंग हो सकती है, जो प्राइवेसी के अधिकार का उल्लंघन कर सकता है

सर्वोच्च न्यायालय (2017) ने कहा है कि प्राइवेसी के अधिकार का कोई भी उल्लंघन, ऐसी दखल की जरूरत के अनुपात में होना चाहिए।[1] राज्य के लिए छूट से डेटा कलेक्शन, प्रोसेसिंग और रिटेंशन, उससे अधिक हो सकता है, जितना जरूरी है। यह आनुपातिक नहीं हो सकता है, और प्राइवेसी के मौलिक अधिकार का उल्लंघन कर सकता है।

बिल केंद्र सरकार को अधिकार देता है कि वह कुछ उद्देश्यों के हित में सरकारी एजेंसियों द्वारा प्रोसेसिंग को बिल के किसी एक या सभी प्रावधानों से छूट दे सकती है। ये उद्देश्य हैं, राज्य की सुरक्षा और सार्वजनिक व्यवस्था को बहाल रखना। डेटा प्रिंसिपल्स का कोई भी अधिकार और डेटा फिड्यूशियरीज़ का कोई भी दायित्व (डेटा सुरक्षा को छोड़कर) कुछ मामलों में लागू नहीं होगा जैसे कि अपराधों की रोकथाम, जांच और अभियोजन के लिए प्रोसेसिंग। बिल सरकारी एजेंसियों के लिए यह भी जरूरी नहीं करता कि वे प्रोसेसिंग का उद्देश्य पूरा होने के बाद पर्सनल डेटा को डिलीट कर दें। इन छूटों का इस्तेमाल करते हुए, राष्ट्रीय सुरक्षा के आधार पर, सरकारी एजेंसी नागरिकों से संबंधित डेटा इकट्ठा कर सकती हैं ताकि सर्विलांस के लिए 360 डिग्री प्रोफाइल तैयार किया जा सके। इस उद्देश्य के लिए विभिन्न सरकारी एजेंसियों द्वारा रखे गए डेटा को इस्तेमाल किया जा सकता है। इससे यह प्रश्न उठता है कि क्या ये छूट आनुपातिकता के परीक्षण में खरी उतरेंगी।

राष्ट्रीय सुरक्षा के आधार पर संचार के इंटरसेप्शन के लिए सर्वोच्च न्यायालय (1996) ने विभिन्न सुरक्षात्मक उपायों को अनिवार्य किया था, जिनमें निम्नलिखित शामिल हैं: (i) आवश्यकता स्थापित करना, (ii) उद्देश्य की सीमा, और (iii) स्टोरेज की सीमा।[8,9] ये बिल के तहत डेटा फिड्यूशरीज़ के दायित्वों के समान है जिन्हें लागू करने से छूट दी गई है। श्रीकृष्ण कमिटी (2018) ने सुझाव दिया था कि राष्ट्रीय सुरक्षा और अपराधों की रोकथाम और अभियोजन जैसे आधारों पर प्रोसेसिंग के मामले में, निष्पक्ष और उचित प्रोसेसिंग और सुरक्षा से संबंधित उपायों के अलावा अन्य दायित्व लागू नहीं होने चाहिए।[4] कमिटी ने कहा था कि स्टोरेज की सीमा और उद्देश्य के विवरण जैसे दायित्व, अगर लागू होते हैं तो उन्हें अलग कानून के जरिए लागू किया जाएगा। भारत में ऐसा कोई कानूनी ढांचा नहीं है।

युनाइटेड किंगडम में डेटा प्रोटेक्शन कानून को 2018 में लागू किया गया जोकि राष्ट्रीय सुरक्षा और रक्षा के लिए ऐसी ही छूट देता है।[10] हालांकि इंटेलिजेंस और कानून प्रवर्तन की गतिविधियों के लिए सरकारी एजेंसियों द्वारा पर्सनल डेटासेट्स की बल्क प्रोसेसिंग जैसी कार्रवाइयां इनवेस्टिगेटरी पावर्स एक्ट, 2016 के तहत रेगुलेटेड हैं।[11] इस कार्रवाई के लिए सेक्रेटरी ऑफ स्टेट (यानी गृह मंत्री) द्वारा वॉरंट जारी किया जाता है जिसके लिए ज्यूडीशियल कमीश्नर की पूर्व मंजूरी जरूरी है। ऐसी कार्रवाई के लिए जरूरत और आनुपातिकता स्थापित किए जाने चाहिए। वॉरंट की अवधि के बाद डेटा रिटेंशन पर प्रतिबंध है। यह कानून संसदीय निगरानी के लिए भी प्रावधान करता है।

लाभ, सबसिडी, लाइसेंस और प्रमाणपत्र जैसे उद्देश्यों के लिए सहमति की आवश्यकता न होना क्या उचित है

बिल के अनुसार, जिन मामलों में राज्य लाभ, सेवा, लाइसेंस, परमिट या प्रमाणपत्र के प्रावधान के लिए पर्सनल डेटा की प्रोसेसिंग करता है, उनमें व्यक्ति की सहमति लेना आवश्यक नहीं। बिल विशेष रूप से इनमें से किसी एक उद्देश्य के लिए प्रोसेस किए गए डेटा को दूसरे उद्देश्य के लिए उपयोग करने की अनुमति देता है। वह इनमें से किसी भी उद्देश्य के लिए राज्य के पास पहले से उपलब्ध पर्सनल डेटा के उपयोग की भी अनुमति देता है। इसलिए, यह उद्देश्य की सीमा को हटा देता है, जो प्राइवेसी की सुरक्षा के प्रमुख सिद्धांतों में से एक है। उद्देश्य की सीमा का मतलब है कि डेटा विशिष्ट उद्देश्यों के लिए जमा किया जाना चाहिए, और केवल उसी उद्देश्य के लिए उपयोग किया जाना चाहिए।[4] प्रश्न यह है कि क्या ऐसी छूट उचित हैं।

चूंकि विभिन्न उद्देश्यों के लिए जमा किए गए डेटा को एक साथ जोड़ा जा सकता है, इससे नागरिकों की प्रोफाइलिंग की अनुमति मिल सकती है। दूसरी ओर, अगर सहमति लेने की आवश्यकता होती, तो व्यक्तियों की अपने पर्सनल डेटा के कलेक्शन और शेयरिंग पर स्वायत्तता और नियंत्रण होता।

बिल पर्सनल डेटा की प्रोसेसिंग से होने वाले नुकसान को रेगुलेट नहीं करता

बिल पर्सनल डेटा की प्रोसेसिंग से उत्पन्न होने वाले नुकसानों के जोखिमों को रेगुलेट नहीं करता। श्रीकृष्ण कमिटी (2018) ने कहा था कि नुकसान पर्सनल डेटा प्रोसेसिंग का संभावित परिणाम है।[4] नुकसान में भौतिक नुकसान शामिल हो सकता है, जैसे वित्तीय नुकसान और लाभ या सेवाओं की सुविधा का नुकसान।[4] इसमें आइडेंटिटी की चोरी, प्रतिष्ठा की हानि, भेदभाव और अनुचित सर्विलांस और प्रोफाइलिंग भी शामिल हो सकती है।[4] कमिटी ने सुझाव दिया था कि नुकसान को डेटा प्रोटेक्शन कानून के तहत रेगुलेट किया जाना चाहिए।[4]

पर्सनल डेटा प्रोटेक्शन बिल, 2019 ने नुकसान को निम्नलिखित को शामिल करते हुए परिभाषित किया था: (i) मानसिक आघात, (ii) पहचान की चोरी, (iii) वित्तीय नुकसान, (iv) प्रतिष्ठा का नुकसान, (v) भेदभाव भरा व्यवहार, और (vi) डेटा प्रिंसिपल जिसकी उम्मीद न करे, वैसी निगरानी और सर्विलांस।[12] 2019 का बिल डेटा फिड्यूशरीज़ से यह अपेक्षा करता था कि वे नुकसान के जोखिमों की रोकथाम करें, उसे कम से कम करें और उसका शमन करें।[13] इनमें प्रभाव आकलन और ऑडिट में इन जोखिमों का मूल्यांकन करना शामिल है।[13] यह डेटा प्रिंसिपल को यह अधिकार भी देता था कि अगर उसे कोई नुकसान होता है कि वह डेटा फिड्यूशरी या डेटा प्रोसेसर से क्षतिपूर्ति की मांग कर सकता है।[14] 2019 के बिल की समीक्षा करने वाली ज्वाइंट पार्लियामेंटरी कमिटी ने सुझाव दिया था कि पर्सनल डेटा की प्रोसेसिंग

से उत्पन्न होने वाले नुकसान से संबंधित प्रावधानों को बहाल रखा जाए।[2] यूरोपीय संघ का जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर) भी नुकसान के जोखिम को रेगुलेट करता है और नुकसान की स्थिति में डेटा प्रिंसिपल को क्षतिपूर्ति का प्रावधान करता है।[15]

डेटा पोर्टेबिलिटी और भुला दिए जाने का अधिकार नहीं देता

बिल डेटा पोर्टेबिलिटी का अधिकार और राइट टु बी फॉरगॉटन नहीं देता। 2018 का ड्राफ्ट बिल और संसद में पेश किया गया 2019 का बिल इन अधिकारों का प्रावधान करता था।[16,17] 2019 के बिल की समीक्षा करने वाली ज्वाइंट पार्लियामेंटरी कमिटी ने इन अधिकारों को बहाल करने का सुझाव दिया था।[2] जीडीपीआर भी इन अधिकारों को मान्यता देते हैं।[18] श्रीकृष्ण कमिटी (2018) ने कहा था कि डेटा प्रिंसिपल के मजबूत अधिकार डेटा प्रोटेक्शन कानून का अनिवार्य घटक हैं।[4] ये अधिकार स्वायत्तता, पारदर्शिता और जवाबदेही के सिद्धांतों पर आधारित हैं जोकि व्यक्तियों को उनके डेटा पर नियंत्रण प्रदान करते हैं।[4]

डेटा पोर्टेबिलिटी का अधिकार: डेटा पोर्टेबिलिटी का अधिकार डेटा प्रिंसिपल को यह अधिकार देता है कि वह एक संरचित, आमतौर पर उपयोग किए जाने वाले और मशीन-रीडेबल फॉरमैट में अपने खुद के उपयोग के लिए डेटा फिड्यूशरी से अपना डेटा हासिल कर सकता है और उसे ट्रांसफर करवा सकता है। यह डेटा प्रिंसिपल को उनके डेटा पर अधिक नियंत्रण देता है। यह एक डेटा फिड्यूशरी से दूसरे में डेटा के ट्रांसफर की सुविधा प्रदान कर सकता है। एक संभावित चिंता यह है कि इससे डेटा फिड्यूशरी के ट्रेड सीक्रेट्स का खुलासा हो सकता है।[4] श्रीकृष्ण कमिटी (2018) ने सुझाव दिया था कि जिस हद तक इन ट्रेड सीक्रेट्स को उजागर किए बिना जानकारी प्रदान करना संभव है, अधिकार की गारंटी दी जानी चाहिए।[4] ज्वाइंट पार्लियामेंटरी कमिटी ने कहा था कि ट्रेड सीक्रेट्स डेटा पोर्टेबिलिटी के अधिकार से इनकार का आधार नहीं हो सकते हैं और केवल तकनीकी व्यावहारिकता के आधार पर इससे इनकार किया जा सकता है।[2]

भुला दिए जाने का अधिकार (राइट टु बी फॉरगॉटन): भुला दिए जाने के अधिकार का अर्थ है, इंटरनेट पर अपने पर्सनल डेटा के खुलासे को सीमित करने का अधिकार।[4] श्रीकृष्ण कमिटी (2018) ने कहा था कि भुला दिए जाने का अधिकार एक विचार है जोकि अन्यथा असीमित डिजिटल स्पेस में स्मृति की सीमाओं को स्थापित करने का प्रयास करता है।[4] हालांकि कमिटी ने इस बात पर भी प्रकाश डाला कि इस अधिकार को प्रतिस्पर्धी अधिकारों और हितों के साथ संतुलित करने की आवश्यकता हो सकती है। इस अधिकार का प्रयोग किसी अन्य के बोलने और अभिव्यक्ति की स्वतंत्रता के अधिकार और सूचना प्राप्त करने के अधिकार में हस्तक्षेप कर सकता है।[1] इसकी एप्लिकेबिलिटी कई कारकों से तय की जा सकती है, जैसे प्रतिबंधित किए जाने वाले पर्सनल डेटा की संवेदनशीलता, जनता के लिए पर्सनल डेटा की प्रासंगिकता और सार्वजनिक जीवन में डेटा प्रिंसिपल की भूमिका।[1]

डेटा के सीमा-पारीय ट्रांसफर के मामले में पर्याप्त सुरक्षा

बिल. क्लॉज 16 (1)

बिल में प्रावधान है कि केंद्र सरकार एक अधिसूचना के माध्यम से कुछ देशों में पर्सनल डेटा के ट्रांसफर को प्रतिबंधित कर सकती है। इसके मायने बिना किसी स्पष्ट नियंत्रण के पर्सनल डेटा को अन्य सभी देशों में ट्रांसफर करना है। प्रश्न यह है कि क्या यह व्यवस्था पर्याप्त सुरक्षा प्रदान करेगी।

भारत के बाहर पर्सनल डेटा के ट्रांसफर के रेगुलेशन का उद्देश्य भारतीय नागरिकों की प्राइवेसी की सुरक्षा करना है।[2] किसी अन्य देश में मजबूत डेटा संरक्षण कानूनों की अनुपस्थिति में, वहां स्टोर किए गए डेटा का ब्रीच का शिकार होने या उनकी विदेशी सरकारों के साथ-साथ निजी संस्थाओं के साथ अनाधिकृत शेयरिंग की अधिक आशंका हो सकती है। 2019 के बिल में यह कहा गया है कि कुछ श्रेणियों के डेटा के लिए किसी देश में ट्रांसफर की अनुमति तभी दी जानी चाहिए, जब वह पर्याप्त स्तर की सुरक्षा प्रदान करता हो।[19] 2022 के ड्राफ्ट बिल ने कुछ अलग नजरिया अपनाया। इसमें केंद्र सरकार को उन देशों को अधिसूचित करना था, जहां पर्सनल डेटा ट्रांसफर किया जा सकता था।[20] इन दोनों व्यवस्थाओं में प्रत्येक देश के मानकों का मूल्यांकन किया जाना था, जहां डेटा का ट्रांसफर किया जाता। देशों को चुनिंदा रूप से प्रतिबंधित करने की व्यवस्था के लिए ऐसे विस्तृत मूल्यांकन की आवश्यकता नहीं है।

नियुक्ति की अल्पावधि बोर्ड की स्वतंत्रता को प्रभावित कर सकती है

बिल. क्लॉज 20 (2)

बिल में प्रावधान है कि भारतीय डेटा प्रोटेक्शन बोर्ड के सदस्य स्वतंत्र निकाय के तौर पर काम करेंगे। सदस्यों को दो वर्षों के लिए नियुक्त किया जाएगा और वे दोबारा नियुक्ति के लिए पात्र होंगे। दोबारा नियुक्ति की गुंजाइश के साथ अल्पावधि का कार्यकाल बोर्ड के स्वतंत्र कामकाज को प्रभावित कर सकता है।

बोर्ड का मुख्य कार्य अनुपालनों की निगरानी करना, जांच करना और सजा पर फैसले सुनाना है। ट्रिब्यूनल्स के मामले में सर्वोच्च न्यायालय (2019) ने कहा था कि अल्पावधि के साथ-साथ पुनर्नियुक्ति के प्रावधानों से कार्यपालिका का प्रभाव और नियंत्रण बढ़ता है।[21] केंद्रीय बिजली रेगुलेटरी आयोग और भारतीय प्रतिस्पर्धा आयोग जैसे निर्णायक भूमिका वाली रेगुलेटरी अथॉरिटीज़ का कार्यकाल संबंधित कानूनों के तहत पांच वर्ष का होता है।[22,23] ट्राई के मामले में नियुक्ति की अवधि तीन वर्ष है।[24] सेबी में नियुक्ति की अवधि पांच वर्ष है जो नियमों के माध्यम से निर्दिष्ट है।[25]

बच्चों के लिए अतिरिक्त प्रावधान

बिल. क्लॉज 2 (एफ) और 9

बच्चों के डेटा की प्रोसेसिंग पर अतिरिक्त दायित्व लागू होते हैं। हम यहां इन प्रावधानों से संबंधित मुद्दों पर चर्चा कर रहे हैं।

बच्चों की परिभाषा अन्य न्यायक्षेत्रों से अलग है

हालांकि यह एक स्वीकृत सिद्धांत है कि बच्चों के डेटा की प्रोसेसिंग अधिक सुरक्षा का विषय होनी चाहिए, लेकिन पर्सनल डेटा की प्रोसेसिंग की सहमति देने के लिए अलग-अलग न्यायक्षेत्रों में बच्चे की परिभाषाएं भिन्न-भिन्न हैं। बिल के तहत एक बच्चा 18 वर्ष से कम आयु के व्यक्ति के रूप में परिभाषित है। यूएसए और यूके में 13 वर्ष से कम आयु के व्यक्ति पर्सनल डेटा की प्रोसेसिंग के लिए अनुमति

दे सकते हैं।[26,27] यूरोपीय संघ का जीडीपीआर इस आयु को 16 वर्ष निर्धारित करता है। सदस्य देश इसे घटाकर 13 वर्ष तक कर सकते हैं।[28] श्रीकृष्ण कमिटी (2018) ने सुझाव दिया था कि बच्चों के लिए सहमति की आयु को निर्धारित करते हुए कुछ कारकों पर विचार किया जाना चाहिए। इनमें निम्नलिखित शामिल हैं: (i) न्यूनतम आयु 13 वर्ष और अधिकतम आयु 18 वर्ष, और (ii) व्यावहारिक कार्यान्वयन सुनिश्चित करने के लिए एकल सीमा।[4] यह भी देखा गया कि बच्चे के पूर्ण स्वायत्त विकास के दृष्टिकोण से 18 वर्ष बहुत अधिक हो सकते हैं।[4] हालांकि मौजूदा कानूनी ढांचे के अनुरूप होने के लिए सहमति की आयु 18 वर्ष होनी चाहिए।[4] भारतीय कॉन्ट्रैक्ट एक्ट, 1872 के तहत कॉन्ट्रैक्ट्स पर हस्ताक्षर करने की न्यूनतम आयु 18 वर्ष है।[29]

माता-पिता से सत्यापन योग्य सहमति लेने के लिए डिजिटल प्लेटफॉर्म पर सभी की आयु के सत्यापन की आवश्यकता हो सकती है

बिल के तहत सभी डेटा फिड्यूशरीज़ को किसी बच्चे के पर्सनल डेटा की प्रोसेसिंग से पहले कानूनी अभिभावक से सत्यापन योग्य सहमति प्राप्त करनी आवश्यक है। इस प्रावधान का अनुपालन करने के लिए प्रत्येक डेटा फिड्यूशरी को उसकी सेवाओं के लिए साइन-अप करने वाले प्रत्येक व्यक्ति की आयु सत्यापित करनी होगी। यह निर्धारित करने की आवश्यकता होगी कि व्यक्ति बच्चा है या नहीं और इस प्रकार उनके कानूनी अभिभावक से सहमति प्राप्त की जाएगी। इससे बच्चों द्वारा झूठी घोषणा करने के मामले से बचने में मदद मिल सकती है। हालांकि इससे डिजिटल क्षेत्र में गुमनामी (एनॉनिमिटी) कम हो सकती है।

बच्चों के हित के लिए क्या नुकसानदेह हो सकता है, इसकी स्पष्टता की कमी

बिल में प्रावधान है कि डेटा फिड्यूशरी ऐसी कोई प्रोसेसिंग नहीं करेगी जिसका बच्चे के हित पर हानिकारक प्रभाव पड़े। बिल में हानिकारक प्रभाव को परिभाषित नहीं किया गया है। यह ऐसे प्रभाव को निर्धारित करने के लिए कोई मार्गदर्शन भी प्रदान नहीं करता है।

सहमति के लिए नोटिस से छूट उचित नहीं हो सकती

बिल: क्लॉज 5, 6, 17 (3)

बिल केंद्र सरकार को यह अधिकार देता है कि वह स्टार्टअप्स सहित कुछ डेटा फिड्यूशरीज़ या डेटा फिड्यूशरीज़ के वर्गों को कुछ दायित्वों से छूट दे सकती है। यह पर्सनल डेटा की मात्रा और प्रकृति को ध्यान में रखते हुए किया जाना चाहिए। जिन दायित्वों से छूट दी जा सकती है, उनमें से एक सहमति के लिए नोटिस है। इन संस्थाओं के मामले में निःशुल्क और सूचित सहमति लेने की आवश्यकता लागू रहेगी। हालांकि अगर जमा किए गए डेटा की प्रकृति और प्रोसेसिंग के उद्देश्य के बारे में नोटिस देने की कोई बाध्यता नहीं है तो यह तर्क दिया जा सकता है कि डेटा प्रिंसिपल सूचित सहमति देने में सक्षम नहीं होगा।

ड्राफ्टिंग के मुद्दे

बिल: क्लॉज 27 (1) (ई), 36

क्लॉज 27 (1) (ई) क्लॉज 36 के सब-सेक्शन (2) का संदर्भ देता है, हालांकि क्लॉज 36 में ऐसा कोई सब-सेक्शन नहीं है।

डेटा प्रोटेक्शन कानून के विभिन्न ड्राफ्ट्स के बीच मुख्य अंतर

तालिका 1: डेटा प्रोटेक्शन कानून के विभिन्न ड्राफ्ट्स की तुलना

ड्राफ्ट पर्सनल डेटा प्रोटेक्शन बिल, 2018	पर्सनल डेटा प्रोटेक्शन बिल, 2019	ज्वाइंट पार्लियामेंटरी कमिटी के सुझाव	डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2023
दायरा और एप्लिकेबिलिटी			
▪ पर्सनल डेटा की प्रोसेसिंग: (i) भारत के भीतर, (ii) भारत के बाहर, अगर वह भारत में बिजनेस करने, वस्तुओं और सेवाओं को पेश करने या व्यक्तियों की प्रोफाइलिंग के लिए की जाती है।	▪ 2018 के बिल का दायरा बढ़ाता है जिससे कुछ निर्दिष्ट अनाम पर्सनल डेटा को इसमें शामिल किया जा सके।	▪ 2018 के बिल के दायरे को बढ़ाया जाए जिससे उसमें नॉन-पर्सनल डेटा और अनाम पर्सनल डेटा की प्रोसेसिंग को शामिल किया जा सके।	▪ ऑफलाइन पर्सनल डेटा और नॉन-ऑटोमेटेड प्रोसेसिंग शामिल नहीं।
डेटा ब्रीच की जानकारी			
▪ फिड्यूशरी डेटा प्रोटेक्शन अथॉरिटी को उस ब्रीच की जानकारी देगा, जिससे नुकसान की आशंका है, अथॉरिटी तय करेगी कि डेटा प्रिंसिपल को इसकी सूचना देनी है या नहीं।	▪ 2018 के बिल के समान।	▪ सभी प्रकार के ब्रीच, भले ही वह नुकसानदेह न हो, की जानकारी अथॉरिटी को 72 घंटे के भीतर दी जानी चाहिए।	▪ हर पर्सनल डेटा ब्रीच की सूचना भारतीय डेटा प्रोटेक्शन बोर्ड और प्रत्येक प्रभावित डेटा प्रिंसिपल को एक निर्दिष्ट तरीके से दी जानी चाहिए।
राज्य की सुरक्षा, सार्वजनिक व्यवस्था, अपराधों की रोकथाम इत्यादि के लिए बिल के प्रावधानों से छूट			
▪ प्रोसेसिंग को कानून के अनुसार और कानून द्वारा स्थापित प्रक्रिया के अनुसार अधिकृत किया जाना चाहिए, और आवश्यक और आनुपातिक होना चाहिए।	▪ केंद्र सरकार, आदेश द्वारा, उन एजेंसियों को छूट दे सकती है जहां प्रोसेसिंग आवश्यक या उचित है जोकि कुछ प्रक्रियाओं,	▪ यह जोड़ा कि आदेश में एक प्रक्रिया निर्दिष्ट होनी चाहिए, जो निष्पक्ष, न्यायसंगत और उचित हो।	▪ केंद्र सरकार एक अधिसूचना के जरिए छूट दे सकती है, इसके लिए किसी प्रक्रिया या सुरक्षात्मक उपायों को निर्दिष्ट करने की जरूरत नहीं है।

	सुरक्षा उपायों और निरीक्षण के अधीन होगा।		
डेटा पोर्टेबिलिटी का अधिकार और भुला दिए जाने का अधिकार			
▪ डेटा प्रिंसिपल को डेटा पोर्टेबिलिटी (इंटरऑपरेबल फॉरमैट में डेटा को हासिल करना) का अधिकार और भुला दिए जाने का (इंटरनेट पर पर्सनल डेटा के खुलासे को सीमित करना) अधिकार होगा।	▪ दोनों अधिकारों का प्रावधान।	▪ दोनों अधिकारों का प्रावधान।	▪ प्रावधान नहीं।
पर्सनल डेटा की प्रोसेसिंग से होने वाला नुकसान			
▪ नुकसान में मौद्रिक हानि, पहचान की चोरी, प्रतिष्ठा की हानि और अनुचित सर्विलांस शामिल है। ▪ डेटा फिड्यूशरी को नुकसान के जोखिमों को कम करने और हल्का करने के लिए उपाय करने होंगे। ▪ डेटा प्रिंसिपल को नुकसान की स्थिति में क्षतिपूर्ति मांगने का अधिकार है।	▪ 2018 के बिल के समान।	▪ केंद्र सरकार को अतिरिक्त नुकसानों को निर्दिष्ट करने का अधिकार होना चाहिए।	▪ प्रावधान नहीं।
रेगुलेटर			
▪ निम्नलिखित की स्थापना का प्रावधान है: (i) क्षेत्र को रेगुलेट करने के लिए भारतीय डेटा प्रोटेक्शन अथॉरिटी, और (ii) अपीलीय ट्रिब्यूनल।	▪ 2018 के बिल के समान।	▪ 2018 के बिल के समान।	▪ भारतीय डेटा प्रोटेक्शन बोर्ड का प्रावधान है जिसका मुख्य कार्य गैर अनुपालन पर फैसले देना है। ▪ अपीलीय ट्रिब्यूनल के तौर पर टीडीसैट नामित।
भारत के बाहर पर्सनल डेटा का ट्रांसफर			
▪ हर फिड्यूशरी को पर्सनल डेटा की कम से कम एक सर्विंग कॉपी भारत में स्टोर करनी होगी। ▪ अगर सहमति दी जाती है, तो भारत के बाहर कुछ निश्चित देशों में या अथॉरिटी द्वारा अनुमोदित अनुबंधों के तहत ट्रांसफर किया जा सकता है। ▪ कुछ महत्वपूर्ण डेटा केवल भारत में ही प्रोसेस किए जा सकते हैं।	▪ संवेदनशील पर्सनल डेटा की एक कॉपी भारत में रहनी चाहिए। ▪ कुछ संवेदनशील पर्सनल डेटा केवल तभी ट्रांसफर किया जा सकता है जब स्पष्ट सहमति प्रदान की गई हो, अन्य पर्सनल डेटा पर कोई प्रतिबंध नहीं है। ▪ महत्वपूर्ण पर्सनल डेटा पर, 2018 बिल के समान।	▪ कहा गया कि संवेदनशील पर्सनल डेटा को केंद्र सरकार की पूर्व मंजूरी के बिना विदेशी एजेंसियों या सरकार के साथ शेयर नहीं किया जाएगा।	▪ संवेदनशील और महत्वपूर्ण पर्सनल डेटा के वर्गीकरण को हटाता है। ▪ केंद्र सरकार अधिसूचना के माध्यम से पर्सनल डेटा को कुछ देशों तक सीमित कर सकती है।

स्रोत: ड्राफ्ट पर्सनल डेटा प्रोटेक्शन बिल, 2018; लोकसभा में पेश किए गए पर्सनल डेटा प्रोटेक्शन बिल, 2019 और डिजिटल पर्सनल डेटा प्रोटेक्शन बिल, 2023; पर्सनल डेटा प्रोटेक्शन बिल, 2019 पर ज्वाइंट पार्लियामेंटरी कमिटी की रिपोर्ट; पीआरएस।

1. Justice K.S. Puttaswamy (Retd) vs. Union of India, W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017.
2. Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021.
3. The Information Technology Act, 2000.
4. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 2018.
5. The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
6. The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
7. The Digital Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
8. Rule 419A, The Indian Telegraph Rules, 1951 issued under Section 7 (2) of the Indian Telegraph Act, 1885.
9. People's Union for Civil Liberties (PUCL) vs Union of India, Supreme Court of India, December 18, 1996.
10. Chapter 3, Data Protection Act, 2018, United Kingdom.
11. Part 6, 7, and 8, Investigatory Powers Act, 2016, United Kingdom.
12. Clause 2 (20), Clause 2 (38), Clause 15, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.

13. Clause 22, Clause 23, Clause 26, Clause 27, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
14. Clause 64, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
15. Recital 75, Article 82, General Data Protection Regulation of European Union.
16. Clause 26, The Personal Data Protection Bill, 2018, as released by Ministry of Electronics and Information Technology.
17. Clause 19, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
18. Article 20, General Data Protection Regulation, European Union.
19. Clause 33 and 34, The Personal Data Protection Bill, 2019, as introduced in Lok Sabha.
20. Clause 17, The Draft Digital Personal Data Protection Bill, 2022, Ministry of Electronics and Information Technology, November 18, 2022.
21. Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.), Supreme Court of India, November 13, 2019.
22. Section 89, The Electricity Act, 2003.
23. Section 10 (1), The Competition Act, 2002.
24. Section 5 (2), The Telecom Regulatory Authority of India Act, 1997.
25. Rule 3 (2), The SEBI (Terms and Conditions of Service of Chairman and Members) Rules, 1992.
26. Children's Online Privacy Protection Rule ("COPPA"), Federal Trade Commission, USA, as accessed on December 6, 2022.
27. Guide to Data Protection, Information, Information Commissioner's Office, United Kingdom, as accessed on December 6, 2022.
28. Article 8, General Data Protection Regulation, European Union.
29. Section 11, The Indian Contract Act, 1872.